

ORIGINAL

UNITED STATES DISTRICT COURT

for the
Central District of CaliforniaIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)Safe Deposit Box 2105, U.S. Private Vaults, 9182 West
Olympic Boulevard, Beverly Hills, California 90212

Case No.

15-2035M

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search
of the following person or property located in the Central District of California
(identify the person or describe the property to be searched and give its location):

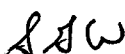
See Attachment A

The person or property to be searched, described above, is believed to conceal (identify the person or describe the
property to be seized):

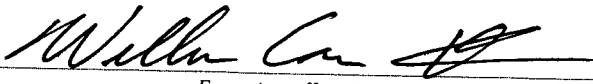
See Attachment B

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or
property. Such affidavit is attached hereto and incorporated herein by reference.**YOU ARE COMMANDED** to execute this warrant on or before 14 days from the date of its issuance
(not to exceed 14 days)☒ in the daytime 6:00 a.m. to 10 p.m. ☐ at any time in the day or night as I find reasonable cause has been
established.Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property
taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the
place where the property was taken.The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an
inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge
on duty at the time of the return through a filing with the Clerk's Office.

(name)

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay
of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be
searched or seized (check the appropriate box) ☐ for _____ days (not to exceed 30).☐ until, the facts justifying, the later specific date of _____.Date and time issued: 10.26.2015
12:15 PM
Judge's signatureCity and state: Los Angeles, CaliforniaHon. Andrew J. Wistrich, U.S. Magistrate Judge
Printed name and title

AO 93 (Rev. 12/09) Search and Seizure Warrant (Page 2)

Return		
Case No.: 15-20351	Date and time warrant executed: OCTOBER 28, 2015 AT 10:07AM	Copy of warrant and inventory left with: IN SAFE DEPOSIT BOX
Inventory made in the presence of: GEORGE VASQUEZ, USPU CONCIERGE		
Inventory of the property taken and name of any person(s) seized: [Please provide a description that would be sufficient to demonstrate that the items seized fall within the items authorized to be seized pursuant to the warrant (e.g., type of documents, as opposed to "miscellaneous documents") as well as the approximate volume of any documents seized (e.g., number of boxes). If reference is made to an attached description of property, specify the number of pages to the attachment and any case number appearing thereon.]		
<ol style="list-style-type: none"> 1. \$500,000 IN US CURRENCY 2. ONE (1) BOX CONTAINING 15 GOLD COLORED COINS AND 22 GOLD COLORED BARS 3. TWO (2) DOCUMENTS - ONE (1) GOLDFELLAS RECEIPT AND ONE (1) US PRIVATE VAULTS PRICE LIST 		
Certification (by officer present during the execution of the warrant)		
I declare under penalty of perjury that I am an officer who executed this warrant and that this inventory is correct and was returned along with the original warrant to the designated judge through a filing with the Clerk's Office.		
Date: 10/29/2015	 Executing officer's signature WILLIAM CONE, SPECIAL AGENT, FBI Printed name and title	

ATTACHMENT A

PREMISES TO BE SEARCHED

Premises known and described as Safe Deposit Box 2105, which is located and maintained at the store front vault business identified as U.S. Private Vaults, located at 9182 West Olympic Boulevard, Beverly Hills, California 90212-3540 (SUBJECT PREMISES 4). The store front is located in a strip mall on the south side of West Olympic Boulevard, west of South Oakhurst Dr., and east of South Palm Drive. The store has glass front windows with a lighted sign above the front door that reads "U.S. Private Vaults" in blue and red colors. The front door faces north toward West Olympic Boulevard and has the address "9182" displayed on the front door. SUBJECT PREMISES 4 is located inside the business and is constructed with a metal type of material, has a shiny metallic color, has a key lock on the front, and has the box number "2105" displayed on the front of the box.

ATTACHMENT B

I. Items to be seized

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of conducting an illegal gambling business, in violation of 18 U.S.C. § 1955; ~~interstate and foreign travel or transportation in aid of racketeering enterprise, in violation of~~ 18 U.S.C. § 1952; transmission of wagering information, in violation of 18 U.S.C. § 1084; money laundering, in violation of 18 U.S.C. §§ 1956 and 1957; and conspiracy in violation of 18 U.S.C. § 371:

a. Any records, documents, programs, applications, or materials describing or constituting an illegal gambling business, including wagering paraphernalia consisting of sports information papers and line sheets; books of accounts; financial records (including but not limited to, bank statements, cancelled checks, ledgers, receipts, tax returns, real property documents, wire and other fund transfer records); monetary instruments; safe deposit documents and keys; safes, telephone books and address books; telephones and wireless telephones; checks; money orders; cash; financial records; notes; betting slips, tally sheets or controller sheets, ledgers or logs, and account books; settlement figures; summary sheets; betting slips; code names of clients; names and/or aliases of businesses used to ~~conceal their illegal gambling business;~~

b. Any digital device used to facilitate the above-listed violations and forensic copies thereof;

c. With respect to any digital device used to facilitate the above-listed violations or containing evidence falling within the scope of the foregoing categories of items to be seized:

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted between February 2014 and the present, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

i. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

ii. evidence of the attachment of other devices;

iii. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

iv. evidence of the times the device was used between February 2014 and the present;

v. passwords, encryption keys, and other access devices that may be necessary to access the device;

vi. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

vii. records of or information about Internet Protocol addresses used by the device;

viii. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or

“favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. As used herein, the terms “records”, “documents”, “programs”, “applications” and “materials” include records, documents, programs, applications or materials created, ~~modified or stored in any form, including in digital form on any digital device and any~~ forensic copies thereof.

3. As used herein, the term “digital device” includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

II. SEARCH PROCEDURE FOR DIGITAL DEVICES

4. In searching digital devices or forensic copies thereof, law enforcement ~~personnel executing this search warrant will employ the following procedure:~~

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the “search team”) will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) to an appropriate law enforcement laboratory or similar facility to be searched at that location. The search team shall complete

the search as soon as is practicable but not to exceed 60 days from the date of execution of the warrant. If additional time is needed, the government may seek an extension of this time period from the Court on or before the date by which the search was to have been completed.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the device and any data thereon falls within the list of items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the list of items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

c. When searching a digital device pursuant to the specific search protocols selected, the search team shall make and retain notes regarding how the search was conducted pursuant to the selected protocols.

d. If the search team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

e. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

f. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

g. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of items to be seized, the government may retain forensic copies of the digital device but may not access them (after the time for searching the device has expired) absent further court order.

h. The government may retain a digital device itself until further order of the Court or one year after the conclusion of the criminal investigation or case (whichever is latest), only if the device is determined to be an instrumentality of an offense under investigation or the government, within 14 days following the time period authorized by the Court for completing the search, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending). Otherwise, the government must return the device.

i. Notwithstanding the above, after the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

5. In order to search for data capable of being read or interpreted by a digital device, law enforcement personnel are authorized to seize the following items:

a. Any digital device capable of being used to commit, further or store evidence of the offense(s) listed above;

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

6. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.